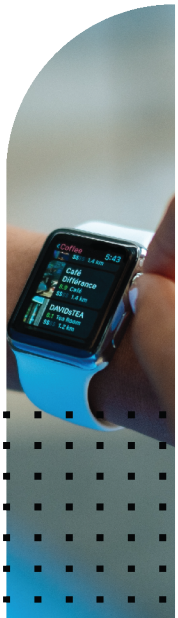
Release Notes

FortiSwitchOS 7.0.4



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

June 13, 2022
FortiSwitchOS 7.0.4 Release Notes
11-704-774657-20220613

TABLE OF CONTENTS

Change log

Date	Change Description
March 4, 2022	Initial release for FortiSwitchOS 7.0.4
March 7, 2022	Added bug 788021 as a resolved issue.
June 13, 2022	Added bug 667079 as a known issue.

Introduction

This document provides the following information for FortiSwitchOS 7.0.4 build 0071.

See the Fortinet Document Library for FortiSwitchOS documentation.

Supported models

FortiSwitchOS 7.0.4 supports the following models:

FortiSwitch 1xx	FS-108E, FS-108E-POE, FS-108E-FPOE, FS-108F, FS-108F-POE, FS-108F-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-124F, FS-124F-POE, FS-124F-FPOE, FS-148E, FS-148E-POE, FS-148F, FS-148F-POE, FS-148F-FPOE
FortiSwitch 2xx	FS-224D-FPOE, FS-224E, FS-224E-POE, FS-248D, FS-248E-POE, FS-248E-FPOE
FortiSwitch 4xx	FS-424D, FS-424D-FPOE, FS-424D-POE, FS-424E, FS-424E-POE, FS-424E-FPOE, FS-424E-Fiber, FS-M426E-FPOE, FS-448D, FS-448D-FPOE, FS-448D-POE, FS-448E, FS-448E-POE, FS-448E-FPOE
FortiSwitch 5xx	FS-524D-FPOE, FS-524D, FS-548D, FS-548D-FPOE
FortiSwitch 1xxx	FS-1024D, FS-1024E, FS-1048D, FS-1048E, FS-T1024E
FortiSwitch 3xxx	FS-3032D, FS-3032E
FortiSwitch Rugged	FSR-112D-POE, FSR-124D

What's new in FortiSwitchOS 7.0.4

Release 7.0.4 provides the following new features:

- Administrators can now use the following commands to control whether users can log in with the FortiSwitchOS console port:

```
config system console
       set login {enable | disable}
end
```

  By default, users can log in with the FortiSwitchOS console port.
- You can now set the speed of ports 21-28 of the FSR-124D model to 100 Mbps full-duplex (`100full`) and 100 MBps half-duplex (`100half`) to support the 100Base-FX module:

```
config switch physical-port
       edit port {port21-port28}
              set speed {auto | 100full | 100half | 1000full | 1000auto}
       next
end
```

- You can now change how long the FortiSwitch CPU usage must be higher than the specified threshold before an SNMP v3 notification (trap) is reported.

```
config system snmp sysinfo
       set trap-high-cpu-interval {1min | 10min | 30min | 1hr | 12hr | 24hr}
end
```

Refer to the FortiSwitch feature matrix for details about the features supported by each FortiSwitch model.

Special notices

Downgrading FortiSwitchOS 7.0.0 and later to versions earlier than 6.2.6 or 6.4.4 is not supported

Downgrading FortiSwitchOS 7.0.0 and later to FortiSwitchOS 6.2.6 and later 6.2 versions is supported. Downgrading FortiSwitchOS 7.0.0 and later to FortiSwitchOS 6.4.4 and later 6.4 versions is supported. Downgrading FortiSwitchOS 7.0.0 to versions earlier than FortiSwitchOS 6.2.6 or 6.4.4 is not supported.

Downgrading FortiSwitchOS 7.0.0 and later requires converting the admin password first

Because FortiSwitchOS 7.0.0 changed from SHA1 to SHA256 encryption for admin passwords, you need to convert the format of the admin password before downgrading from FortiSwitchOS 7.0.0 and later to an earlier FortiSwitchOS version.

If you do not convert the admin password before downgrading from FortiSwitchOS 7.0.0 and later, the admin password will not work after the switch reboots with the earlier FortiSwitchOS version.

The encrypted admin password in FortiSwitchOS 7.0.0 and higher starts with “SH2”, and the encrypted admin password for earlier FortiSwitchOS versions starts with “AK1”.

To convert the format of the admin password in FortiSwitchOS 7.0.0 and later before downgrading to an earlier FortiSwitchOS version:

1. Enter the following CLI command to convert the admin password from SHA256 to SHA1 encryption:

   ```
   execute system admin account-convert <admin_name>
   ```

2. Downgrade your firmware.

Connecting multiple FSR-112D-POE switches

The FSR-112D-POE switch does not support interconnectivity to other FSR-112D-POE switches using the PoE ports. Fortinet recommends using the SFP ports to interconnect switches.

Upgrade information

FortiSwitchOS 7.0.4 supports upgrading from FortiSwitchOS 3.5.0 and later.

For FortiSwitch units managed by FortiGate units, refer to the *FortiSwitch Devices Managed by FortiOS Release Notes* for upgrade information. See https://docs.fortinet.com/document/fortiswitch/7.0.0/managed-switch-release-notes.

Product integration and support

FortiSwitchOS 7.0.4 support

The following table lists FortiSwitchOS 7.0.4 product integration and support information.

Web browser	• Mozilla Firefox version 52 • Google Chrome version 56 Other web browsers may function correctly, but are not supported by Fortinet.
FortiOS (FortiLink Support)	FortiLink is supported on all FortiSwitch models when running FortiOS 5.4.0 and later and FortiSwitchOS 3.2.1 and later.

Resolved issues

The following issues have been fixed in FortiSwitchOS 7.0.4. For inquiries about a particular bug, please contact Customer Service & Support.

734917	When you configure a PIM multicast flow with a range of group addresses for SVIs and the group address range overlaps with a dynamic IGMPv3 group receiver that has joined groups in a different VLAN, then the dynamic IGMPv3 receiver will still receive multicast traffic unexpectedly even after leaving the joined groups.
748210	The MAC authentication bypass (MAB) sometimes does not work on the FS-424E when a third-party hub is disconnected and then reconnected.
759992	After restarting the FortiSwitch unit, memory usage increases, and the user cannot access the FortiSwitch unit with the CLI or GUI.
760536	The SNMP trap for monitoring the power supply failure and restoration is using the wrong object identifier (OID).
763953	After LDAP authentication is successful, the admin user cannot log in.
765197	The automatic topology creates an ISL trunk between two switches with the wrong value for the native VLAN.
769733	The getnext query does not work on OID .0/0.0.
770402	The `diagnose switch mclag list` command is reporting a different up time value than the `diagnose switch trunk list` and `get system performance status` commands.
771767	Trusted hosts with a mask other than /32 cannot access the FortiSwitch unit.
776675	• FortiSwitchOS cannot use the NAS-Filter-Rule when it exceeds 65 characters. • If you specify more than one port or port range (for example, `10.105.0.106/24 100,200,300` or `10.105.0.106/24 100-200,300,700-900`) when defining the source or destination in a dynamic ACL entry, FortiSwitchOS applies the first port or port range and ignores the rest. • If you specify the destination port after the `any` keyword, you must specify `any 0.0.0.0/0 <port_number>`. For example, instead of `permit in TCP any to any 90 cnt`, use `permit in TCP any to any 0.0.0.0/0 90 cnt` instead.
783151	There was an error in the definition of fsTrapLlvViolation in the SNMP MIB.
788021	The `poe-pre-standard-detection` setting is shown as disabled in the CLI but enabled on the hardware for the FS-1xxE, FS-1xxF, FS-5xxD, and FSR-112D-POE models.

Common vulnerabilities and exposures

FortiSwitchOS 7.0.4 is no longer vulnerable to the following CVEs:

- CWE-329
- CWE-347
- CWE-916

Visit https://fortiguard.com/psirt for more information.

Known issues

The following known issues have been identified with FortiSwitchOS 7.0.4. For inquiries about a particular bug or to report a bug, please contact Fortinet Customer Service & Support.

Bug ID	Description
382518, 417024, 417073, 417099, 438441	DHCP snooping and dynamic ARP inspection (DAI) do not work with private VLANs (PVLANs).
414972	IGMP snooping might not work correctly when used with 802.1x Dynamic VLAN functionality.
480605	When DHCP snooping is enabled on the FSR-112D-POE, the switched virtual interface (SVI) cannot get the IP address from the DHCP server. **Workarounds:** —Use a static IP address in the SVI when DHCP snooping is enabled on that VLAN. —Temporarily disable dhcp-snooping on vlan, issue the `execute interface dhcpclient-renew <interface>` command to renew the IP address. After the SVI gets the IP address from the DHCP server, you can enable DHCP snooping.
510943	The time-domain reflectometer (TDR) function (cable diagnostics feature) reports unexpected values. **Workaround:** When using the cable diagnostics feature on a port (with the `diagnose switch physical-ports cable-diag <physical port name>` CLI command), ensure that the physical link on its neighbor port is down. You can disable the neighbor ports or physically remove the cables.
542031	For the 5xx switches, the `diagnose switch physical-ports led-flash` command flashes only the SFP port LEDs, instead of all the port LEDs.
548783	Some models support setting the mirror destination to “internal.” This is intended only for debugging purposes and might prevent critical protocols from operating on ports being used as mirror sources.
572052	Backup files from FortiSwitchOS 3.x that have 16-character-long passwords fail when restored on FortiSwitchOS 6.x. In FortiSwitchOS 6.x, file backups fail with passwords longer than 15 characters. **Workaround:** Use passwords with a maximum of 15 characters for FortiSwitchOS 3.x and 6.x.
585550	When packet sampling is enabled on an interface, packets that should be dropped by uRPF will be forwarded.

Bug ID	Description
606044/610149	The results are inaccurate when running cable diagnostics on the FS-108E, FS-124E, FS-108E-POE, FS-108E-FPOE, FS-124E-POE, FS-124E-FPOE, FS-148E, and FS-148E-POE models.
609375	The FortiSwitchOS supports four priority levels (critical, high, medium, and low); however, The SNMP Power Ethernet MIB only supports three levels. To support the MIB, a power priority of medium is returned as low for the PoE MIB.
667079	For the FSR-112D-POE model: • If you have enabled IGMP snooping or MLD snooping, the FortiSwitch unit does not support IPv6 functionalities and cannot pass IPv6 protocol packets transparently. • If you want to use IGMP snooping or MLD snooping with IPv6 functionalities, you need to enable `set flood-unknown-multicast` under the `config switch global` command.
673433	Some 7-meter DAC cables cause traffic loss for the FS- 448E model.
724813	The `set enforce-first-as {disable | enable}` command should have been placed under `config neighbor` and does not work in its current location (directly under `config router bgp`). There is no patch available for this issue.
784585	When a dynamic LACP trunk has formed between switches in an MRP ring, the MRP ring cannot be closed. Deleting the dynamic LACP trunk does not fix this issue. MRP supports only physical ports and static trunks; MRP does not support dynamic LACP trunks. **Workaround:** Disable MRP and then re-enable MRP.

www.fortinet.com